UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

RICHARD MATERNA, on behalf of himself and all others similarly situated,

Plaintiff,

v.

CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE, N.A, CAPITAL ONE BANK (USA), N.A., AMAZON.COM, INC., and AMAZON WEB SERVICES, INC.,

Defendants.

CLASS ACTION COMPLAINT

JURY TRIAL DEMAND

3:19cv581

Plaintiff Richard Materna ("Plaintiff"), by his undersigned counsel, brings this class action on behalf of himself and a class of all others similarly situated against Defendants Amazon.com, Inc. and Amazon Web Services, Inc. ("AWS") (collectively, the "Amazon Defendants") and Capital One Financial Corporation, Capital One, N.A., and Capital One Bank (USA), N.A., (collectively, the "Capital One Defendants" or "Capital One"). Plaintiff alleges the following based upon personal information and belief, the investigation of counsel, and states the following:

I. INTRODUCTION

1. This action arises out of the data breach announced by Capital One on July 29, 2019, wherein Personally Identifiable Information ("PII") of more than 100 million consumers was illegally obtained by a hacker after gaining unauthorized access to Capital One data being stored on AWS' cloud servers (the "Capital One Data Breach").

2. On July 19, 2019, Capital One "determined there was unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for its credit card products and to Capital One credit card customers."[1] The Federal Bureau of Investigations ("FBI") corroborated this information and further stated that "[a] firewall misconfiguration permitted commands to reach and be executed by [an AWS] server, which enabled access to folders or buckets of data in Capital One's storage space"[2] on AWS' cloud.

3. The Capital One Data Breach resulted in more than 100 million Capital One consumers' PII being exfiltrated on or around March and April 2019, including names, mailing addresses, zip/postal codes, phone numbers, email addresses, dates of birth, self-reported income, social security numbers, and linked bank account numbers to secured credit card customers.

4. Through its failure to adequately protect Plaintiff's and the Class members' PII, the Amazon Defendants and Capital One enabled Paige A. Thompson ("Thompson"), a former AWS employee, to obtain access to, copy, remove, and make public Plaintiff's and the Class members' PII.

5. Capital One used the Amazon Defendants' cloud-based services to store the critically sensitive PII of credit applicants.

6. Capital One and the Amazon Defendants failed to adequately protect consumers' PII and did not take reasonable measures to ensure data systems were protected. Specifically, deficiencies in Capital One's firewall enabled Thompson to trick the firewall into relaying requests to a key back-end resource on the AWS platform known as the "metadata" service, which then

[1] *See* Capital One Breach Notification, https://www.capitalone.com/facts2019/ (last accessed Aug. 4, 2019).
[2] *See* Paige A. Thompson Criminal Complaint, Case No. MJ19-0344 ¶ 25 (W.D. Wash.), https://www.justice.gov/usao-wdwa/press-release/file/1188626/download at paragraph 10.

provided Thompson with access to data that Capital One stored on AWS' cloud servers. This vulnerability, of which AWS was previously aware, but which AWS failed to remediate, was an exploitation method known as "Server Side Request Forgery," or SSRF.

7. Through the SSRF attack, Thompson gained access to the PII of consumers and small businesses who applied for one of Capital One's credit card products between 2005 and early 2019. Capital One's inadequate and unreasonable data security procedures and improperly configured firewall, coupled with AWS' inaction on remediating a known cloud platform vulnerability, resulted in Plaintiff and the Class suffering harm as alleged in this Complaint.

8. Despite well-known risks that a data breach could result in widespread harm to consumers, Capital One and the Amazon Defendants failed to act in a reasonable manner to protect consumers' PII.

9. The Capital One and Amazon Defendants also misled consumers about having adequate data security measures, safeguards, infrastructure, and practices to protect consumers' PII in its Notice of Privacy Practices and elsewhere, and failed to safeguard and protect Plaintiff's and the Class members' PII in accordance with federal, state and local laws, and industry standards.

10. Had Capital One informed Plaintiff and Class members that it would not follow federal, state and local laws in protecting their PII, Plaintiff and the Class members would not have provided their PII to Capital One.

11. The Capital One and Amazon Defendants' failures to implement adequate and reasonable data security protocols jeopardized the PII of millions of consumers, fell short of Defendants' promises, obligations, and representations, and failed to live up to Plaintiff's and other Class members' reasonable expectations for protection of the sensitive PII they provided to Capital One, who in turn provided such information to the Amazon Defendants.

12. As a result of the Capital One Data Breach, Plaintiff and Class members' PII has been exposed online for abuse and misuse. Plaintiff and the Class have suffered injuries as a direct and proximate result of the Capital One Data Breach, including theft of personal and financial information, costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts and personal information, costs associated with the time spent and the loss of productivity related to mitigating, monitoring, and managing personal and financial account information in the wake of actual and future consequences of the data breach, including purchasing credit monitoring and identity theft services and identifying fraudulent charges. Plaintiff and the Class have also suffered damages to and diminution in value of their personal and financial information entrusted to Capital One for the sole purpose of obtaining Capital One's products, and now face continued risks that their personal and financial information could result in identity theft and future monetary loss.

13. Plaintiff and the Class seek to remedy these harms and prevent their future occurrence for all similarly situated consumers whose personal and financial information was compromised as a direct and proximate result of the Capital One Data Breach. Consumers seek to recover damages, restitution, disgorgement, equitable relief, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

II. PARTIES

14. Plaintiff Richard Materna is a citizen of Minnesota. In approximately 2013, Plaintiff applied for Visa and MasterCard credit cards offered by Capital One through Capital One's website. In approximately 2018, Plaintiff also applied for a Capital One auto loan online through Capital One's website.

15. Defendant Amazon.com, Inc. is a Delaware corporation and operates its principal place of business in Seattle, Washington.

16. Defendant Amazon Web Services, Inc. is a Delaware corporation and operates its principal place of business in Seattle, Washington. AWS is a subsidiary of Amazon.com, Inc.

17. Defendant Capital One Financial Corporation is a Delaware corporation and operates its principal place of business at 1680 Capital 1 Drive, McLean, Virginia. It offers a broad spectrum of financial products and services to consumers, including credit cards. Capital One Financial Corp. operates through its two primary subsidiaries, Capital One Bank (USA), N.A. and Capital One, N.A.

18. Defendant Capital One Bank (USA), N.A. is a Virginia corporation and operates its principle place of business in McLean, Virginia. Capital One Bank (USA), N.A. is one of Capital One Financial Corporation's two principal subsidiaries. It operates as a bank and offers checking accounts, credit and debit cards, loans, insurance, payment protection, phone banking, bill pay, lending, and online banking services. It primarily serves consumers, small businesses and commercial clients worldwide.

19. Defendant Capital One, N.A. is a Virginia corporation and operates its principle place of business in McLean, Virginia. Capital One, N.A. is the second of Capital One Financial Corporation's two principal subsidiaries. Capital One, N.A. operates as a bank and offers financial products and services such as personal and business checking, savings accounts, investment, mortgages, issues credit card, business loans, and commercial banking solutions. Capital One serves consumers, small businesses, and commercial clients worldwide.

III. JURISDICTION AND VENUE

20. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d). This is a class action in which: (1) there are more than one hundred (100) members in the proposed class; (2) various members of the proposed class are citizens of states different from where Defendants are citizens; and (3) the amount in controversy, exclusive of interest and costs, exceeds $5,000,000 in the aggregate.

21. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

22. This Court has personal jurisdiction over Capital One because they are headquartered in and regularly conduct business in Virginia. Capital One regularly makes corporate decisions, including decisions impacting data storage as well as data security practices, policies, and procedures. Capital One intentionally avails itself of this jurisdiction by eliciting, transacting, and deriving substantial revenues from business activity in this District.

23. This Court also has personal jurisdiction over the Amazon Defendants because the Amazon Defendants conduct business in this District and have sufficient minimum contacts in this District. The Amazon Defendants intentionally avail themselves of this jurisdiction by eliciting, transacting, and deriving substantial revenues from business activities in this district, including negotiating and offering Capital One cloud data storage through its AWS cloud platform.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District and Division. Defendants are also corporations that do business in and are subject to personal jurisdiction in this District and Division.

IV. STATEMENT OF FACTS

A. Capital One's Data Storage Practices

25. Capital One is one of the largest banks in the United States and the fifth-largest U.S. credit card issuer, with $373.6 billion in total assets as of 2019. It specializes in credit cards, but also offers other forms of credit, including automobile loans and a variety of other bank accounts to customers throughout the United States. Capital One solicits potential customers for credit cards and other financial products.

26. To obtain credit from Capital One, consumers must first submit an application to Capital One and provide it with sensitive PII in order for Capital One to determine creditworthiness. Consumers' PII includes their names, addresses, social security numbers, self-reported income, and other valuable, sensitive and private information that lenders and credit reporting agencies use.

27. Plaintiff and the Class rely on Capital One to keep their PII confidential and secure, to use this information solely for business purposes, and to only make disclosures of it as required by law.

28. By obtaining, using, approving, and deriving a benefit from Plaintiff's and the Class' PII, Capital One assumed a legal duty to protect such PII from disclosure.

29. Regardless of whether a credit application is approved or not, Capital One retains consumers' applications, including their PII, on AWS' servers. Based on information and belief, Capital One's common business practice was to retain all documentation, including PII found in loan applications, dating at least as far back as 2005.

30. To store the volume of information Capital One retains, Capital One contracts with AWS for cloud-based storage. AWS' servers provide storage space to Capital One computers that are connected to it via a network or over the internet.

31. The Amazon Defendants provide information technology infrastructure services to businesses such as Capital One. AWS offers a range of services, including Amazon Elastic Compute Cloud ("EC2") and Amazon Simple Storage Service ("Amazon S3" or "S3").[3]

32. Amazon S3 is "an object storage service that offers industry-leading scalability, data availability, security, and performance." S3 enables customers to "store and protect any amount of data." AWS states that S3 provides easy-to-use management features so customers can organize data and configure finely-tuned access controls to meet their specific business, organizational, and compliance requirements.

33. To protect your data in Amazon S3, users only have access to the S3 resources, or "buckets," they create. AWS states that "[b]y default, all Amazon S3 resources—buckets, objects, and related subresources . . . are private: only the resource owner, an AWS account that created it, can access the resource."[4]

34. However, resource owners can grant access to others by using any of the following access management features: AWS Identity and Access Management (IAM) to create users and manage their respective access; Access Control Lists (ACLs) to make individual objects accessible to authorized users; bucket policies to configure permissions for all objects within a single S3 bucket; and Query String Authentication to grant time-limited access to others with temporary

[3] See Amazon Simple Storage Service, https://aws.amazon.com/s3 (last accessed August 1, 2019).
[4] *See* Identity and Access Management in Amazon S3, https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html (last accessed Aug. 5, 2019).

URLs.[5] IAM is the root of all security within AWS and is a foundational tenet of its data security protocol.[6]

B. Capital One and the Amazon Defendants Knew the Importance of Protecting Personal and Financial Information

35. At all relevant times, Capital One knew, or reasonably should have known, that the PII it collects from its credit applications and stored in the cloud is highly sensitive—and sought after—by cyber criminals looking to perpetrate identity theft and fraud. Similarly, the Amazon Defendants knew, or reasonably should have known, that cloud storage data security is fundamental to keeping data secure from hackers on AWS' platform.

36. Both legitimate and criminal organizations alike recognize the importance and value of PII, as that is the information financial institutions use to process and approve consumers for credit cards and other banking products. When PII falls into the hands of identity thieves, they can use that data to open new financial accounts, take out loans in other people's names, incur charges on existing accounts, or clone ATM, debit, and credit cards.

37. Given the sensitive and valuable nature of PII, a "cyber black market" exists where criminals can openly post and obtain stolen payment card numbers, social security numbers, and other personal, private information to perpetrate identity theft and fraud.

38. It is therefore unsurprising that financial institutions are popular targets for cyber attacks, given that the PII financial institutions request to process and approve consumers for credit and other banking products—precisely the information compromised in the Capital One Data Breach—is the PII cyber criminals could use to perpetrate identity theft.

---

[5] *See* Amazon S3 Features, https://aws.amazon.com/s3/features/ (last accessed August 1, 2019).
[6] *See* Preventing the Capital One Breach, https://ejj.io/blog/capital-one (last accessed Aug. 4, 2019).

39. In 2019 alone, there have been 3,494 successful cyber attacks against financial institutions that have been reported to the United States Treasury Department's Financial Crimes Enforcement Network.[7] This, however, is not a new revelation. In "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[8] In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year.[9] And in 2017, Equifax announced a data breach that exposed the personal information of 147 million people,[10] while in 2018 Marriott announced that a data breach exposed personal information of up to 500 million people.[11]

40. Clearly, the PII of consumers remains of high value to cyber criminals, given the pace, scope, and magnitude of breaches that continue to be announced annually.

41. Capital One and the Amazon Defendants knew, or reasonably should have known, of the importance of safeguarding PII, and the foreseeable consequences that would occur if its data security systems were breached, including, specifically, the significant costs that would be imposed on its consumers in the wake of a data breach.

42. Recognizing this significant threat, Capital One sought to assuage consumers by stating "[t]o protect your personal information from unauthorized access and use, we use security

---

[7] *See* Capital One Breach Shows a Bank Hacker Needs Just One Gap to Wreak Havoc, https://www.nytimes.com/2019/07/30/business/bank-hacks-capital-one.html

[8] *See* Verizon 2014 PCI Compliance Report, https://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf

[9] *See* Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout, Identity Theft Resource Center (Jan. 19, 2017), http://www.idtheftcenter.org/2016data-breaches.html.

[10] *See* Equifax Data Breach Settlement, https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement (last accessed Aug. 5, 2019).

[11] *See* The Marriott data breach, https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach (last accessed Aug. 5, 2019).

measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[12] It further states on its website that "[w]e prohibit the unlawful disclosure of your social security number"[13] by "1. Protect[ing] the confidentiality of social security numbers; 2. Prohibit[ing] the unlawful disclosure of social security numbers; and 3. Limit[ing] access to Social Security numbers to employees or others with legitimate business purposes."[14] It also states that "Capital One associates are required to participate in annual security training."[15]

43. Similarly, Amazon recognizes the importance of keeping clients' data protected. AWS makes a public commitment to the security of data stored on its servers:

> At AWS, security is our highest priority. We design our systems with your security and privacy in mind.
>
> - We maintain a wide variety of compliance programs that validate our security controls. Click here to learn more about our compliance programs.
> - We protect the security of your information during transmission to or from AWS websites, applications, products, or services by using encryption protocols and software.
> - We follow the Payment Card Industry Data Security Standard (PCI DSS) when handling credit card data.
> - We maintain physical, electronic, and procedural safeguards in connection with the collection, storage, and disclosure of personal information. Our security procedures mean that we may request proof of identity before we disclose personal information to you.[16]

---

[12] *See* Capital One Privacy Policy, https://www.capitalone.com/bank/privacy/ (last accessed Aug. 5, 2019).
[13] *See* Capital One: Your security is a top priority, https://www.capitalone.com/applications/identity-protection/commitment/#20_pg_sl (last accessed Aug. 5, 2019).
[14] *See* Social Security Number Protections, https://www.capitalone.com/identity-protection/privacy/social-security-number (last accessed Aug. 5, 2019).
[15] *See* Capital One: Bank Securely, https://www.capitalone.com/applications/identity-protection/commitment/#20_pg_sl (last accessed Aug. 5, 2019).
[16] *See* Amazon Privacy Notice https://aws.amazon.com/privacy/ (last accessed Aug. 5, 2019).

C. The Capital One Data Breach

44. On July 29, 2019, Capital One announced that it was the subject of a data breach that affected approximately 100 million individuals via a statement made on its website:

> Date: July 29, 2019
>
> Capital One Financial Corporation (NYSE: COF) announced today that on July 19, 2019, it determined there was unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for its credit card products and to Capital One credit card customers.
>
> Capital One immediately fixed the configuration vulnerability that this individual exploited and promptly began working with federal law enforcement. The FBI has arrested the person responsible. Based on our analysis to date, we believe it is unlikely that the information was used for fraud or disseminated by this individual. However, we will continue to investigate.
> Based on our analysis to date, this event affected approximately 100 million individuals in the United States and approximately 6 million in Canada.
>
> Importantly, no credit card account numbers or log-in credentials were compromised and over 99 percent of Social Security numbers were not compromised.
>
> The largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019. This information included personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income.
>
> Beyond the credit card application data, the individual also obtained portions of credit card customer data, including:
>
> - Customer status data, e.g., credit scores, credit limits, balances, payment history, contact information
> - Fragments of transaction data from a total of 23 days during 2016, 2017 and 2018
>
> No bank account numbers or Social Security numbers were compromised, other than:
>
> - About 140,000 Social Security numbers of our credit card customers
> - About 80,000 linked bank account numbers of our secured credit card customers

- For our Canadian credit card customers, approximately 1 million Social Insurance Numbers were compromised in this incident.

We will notify affected individuals through a variety of channels. We will make free credit monitoring and identity protection available to everyone affected.

Safeguarding applicant and customer information is essential to our mission and our role as a financial institution. We have invested heavily in cybersecurity and will continue to do so. We will incorporate the learnings from this incident to further strengthen our cyber defenses.

The investigation is ongoing and analysis is subject to change.[17]

45. According to Capital One, "[t]he largest category of information accessed was information on consumers and small businesses as of the time they applied for one of [Capital One's] credit card products from 2005 through early 2019."[18] This information included "personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip/postal codes, phone numbers, email addresses, dates of birth, and self-reported income."[19]

46. In addition, Capital One also stated that consumers' credit scores, credit limits, balances, payment histories, contact information, and "fragments of transaction data from a total of 23 days during the 2016, 2017, and 2018" time period were compromised, along with "about 140,000 social security numbers of its credit card customers" and about 80,000 linked bank account numbers of our secured credit customers."[20]

47. The PII compromised in the Capital one Data Breach was due to Capital One's and the Amazon Defendants' acts, omissions, and failure to properly protect PII, despite being aware

[17] *See* Information on the Capital One Cyber Incident, Frequently Asked Questions, Capital One (July 31, 2019), https://www.capitalone.com/facts2019/2/ (last accessed Aug. 5, 2019).
[18] *Id*.
[19] *Id*.
[20] *Id*.

of cybersecurity standards, industry best practices, the propensity financial institutions have to be hacked, and its own proclaimed privacy policies it had in place to prevent precisely this type of breach from happening. Specifically, Capital One failed to adequately safeguard it's network with a properly configured firewall and the Amazon Defendants failed to take steps to mitigate a known SSRF vulnerability on its cloud storage platform, which resulted in Thompson accessing and communicating with servers that should have been off limits to the outside world.

D. The Capital One Data Breach was the Result of Unreasonable Data Security Policies and Practices Carried out by Capital One and the Amazon Defendants

48. The FBI has alleged and charged that Thompson (a/k/a "erratic"), a former systems engineer at AWS, orchestrated the attack. The FBI arrested Thompson on July 29, 2019, and she now faces charges of computer fraud in violation of 18 U.S.C. § 1030(a)(2).

49. Because Thompson is a former Amazon employee at AWS's web services unit, questions exist as to whether she used knowledge acquired while working at the cloud-computing giant to commit the alleged crimes for which she has been charged, says director of cyber-risk research Chris Vickery at the security firm UpGuard, Inc.

50. According to Capital One, Thompson exploited a configuration vulnerability to gain access to the systems. This "unauthorized access also enabled the decrypting of data."[21]

51. However, published reports suggest that Thompson exploited a well-known cloud computing vulnerability known as Server-Side Request Forgery (SSRF) to perform the attack.[22] SSRF attacks occur by tricking a server into running commands that it should never have been

[21] *Id*.
[22] *See* Early Lessons from the Capital One Data Breach, Stratum Security (July 31, 2019) https://blog.stratumsecurity.com/2019/07/31/early-lessons-from-the-capital-one-breach/ (last accessed August 1, 2019).

permitted to run. Both Capital One's and the Amazon Defendants' lackadaisical approach to data security expose them to liability for the Capital One Data Breach.

1. SSRF Attacks: An Overview

52. SSRF vulnerabilities let an attacker send crafted requests from the back-end server of a vulnerable web application. Criminals usually use SSRF attacks to target internal systems that are behind firewalls and are not accessible from the external network.[23]

53. SSRF vulnerabilities occur when an attacker has full or partial control of the request sent by a web application. A common example is when an attacker can control a third-party service URL to which the web application makes a request. By exploiting an SSRF vulnerability, an attacker tricks a server into disclosing sensitive server-side information that would otherwise be inaccessible outside the firewall.[24]

54. Attackers can also use SSRF to make requests to other internal resources that the web server has access to, which are not publicly available. "For example, they can access cloud service instance metadata like AWS/Amazon EC2 and OpenStack."[25]

55. To detect SSRF attacks, companies need to rely on an intermediary service. Detection of such vulnerabilities requires an out-of-band and time-delay vector.[26]

56. There are a variety of ways to mitigate SSRF attacks, including whitelisting DNS names or IP addresses that an application needs to access, disabling unused URL schemas such as "https" or "http" if only one type of URL is used, and authentication on internal services.[27]

---

[23] *See* What is Server Side Request Forgery (SSRF)? (Feb. 20, 2019), https://www.acunetix.com/blog/articles/server-side-request-forgery-vulnerability/ (last accessed Aug. 4, 2019).
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*

57. Reports suggest that Thompson was able to use SSRF to execute a request on an AWS EC2 instance controlled by Capital One that revealed Capital One's AWS S3 credentials.[28] Had Capital One properly secured its network, and had AWS addressed known SSRF vulnerabilities on its cloud platform, Thompson would not have been as successful in breaching and exposing consumers' PII.

2. Capital One's Misconfigured Firewall Gave Thompson Access to its Internal Networks

58. Thompson's SSRF attack was successful due, in part, to a misconfigured Capital One open-source Web Application Firewall ("WAF") that Capital One was using as part of its operations hosted in the AWS cloud.[29]

59. In March 2019, Thompson ran a scan of the internet to find vulnerable computers that could give her access to a company's internal networks. During this scan, Thompson located a Capital One computer server with a misconfigured WAF that was managing communications between the Company's cloud and the public internet.[30]

60. The misconfigured WAF allowed Thompson to access the computer server and trick it into relaying requests to a key back-end resource on the AWS platform known as the "metadata" service, which is responsible for handing out credentials and other data needed to manage servers in the cloud. These credentials are effectively the computer world's equivalent to

---

[28] *Id.*

[29] *See* What We Can Learn from the Capital One Hack (Aug. 2, 2019) https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/ (last accessed Aug. 4, 2019).

[30] *See* How the Accused Capital One Hacker Stole Reams of Data From the Cloud (Aug. 4, 2019) https://www.wsj.com/articles/how-the-accused-capital-one-hacker-stole-reams-of-data-from-the-cloud-11564911001?shareToken=sta69879a3c7c8434698050cd6ca996b4b&reflink=article_email_share (last accessed Aug. 5, 2019).

the keys to a bank vault.[31] Through this exploit, Thompson was able to access whatever credentials that server had access to on AWS' platform.

61. In AWS, exactly what those credentials can be used for hinges on the permissions assigned to the resource that is requesting them. Here, Capital One's misconfigured WAF was assigned too many permissions, i.e. it was allowed to list all of the files in any buckets of data, and to read each of those files.

62. Had Capital One properly configured its WAF and not assigned it too many permissions, Thompson would not have had as wide-ranging access to consumers' PII.

63. As a direct and proximate result of Capital One's inadequate data security measures, its misconfigured firewall, and its insufficient information technology response and scanning protocols, Plaintiff and the Class suffered damages in the form of their PII being exposed.

3. The Amazon Defendants knew of AWS' SSRF Vulnerabilities yet Refuse to Mitigate its Threat

64. SSRF has become the most serious vulnerability facing organizations that use public clouds.[32] According to Scott Piper, who advises companies on their Amazon cloud security, the SSRF vulnerability has been known since at least 2014.[33]

---

[31] *Id*.

[32] Preventing the Capital One Breach, https://ejj.io/blog/capital-one (last Accessed Aug. 4, 2019).

[33] *See* How the Accused Capital One Hacker Stole Reams of Data From the Cloud (Aug. 4, 2019) https://www.wsj.com/articles/how-the-accused-capital-one-hacker-stole-reams-of-data-from-the-cloud-11564911001?shareToken=sta69879a3c7c8434698050cd6ca996b4b&reflink=article_email_share (last accessed Aug. 5, 2019)

65. While SSRF attacks are common and well-known,[34] the Amazon Defendants have failed to correct these known SSRF vulnerabilities, unlike other cloud storage companies such as Google.[35] Significantly, the single-line command that exposes AWS credentials on any EC2 system is known by AWS and is in fact included in their online documentation.[36] It is also well known among hackers.

66. Despite this known vulnerability, Amazon has done nothing to mitigate the threat of it being exploited on AWS' cloud platform. Instead, Amazon considers it its clients' responsibility to address the vulnerability.

67. AWS' SSRF vulnerability is significant and poses a threat to all AWS clients' data. In February 2019, security researcher Brennan Thomas conducted an internet scan and found more than 800 AWS accounts that allowed similar access to the metadata service.[37] Such widespread vulnerability should have demanded action from AWS years ago.

68. On August 5, 2019, U.S. Senator Ron Wyden sent a letter to Amazon seeking answers on its cloud-computing technology at the heart of the Capital One attack. In his letter, he noted that "[w]hen a major corporation loses data on a hundred million Americans because of a configuration error, attention naturally focuses on that corporation's cybersecurity practices . . .

---

[34] *See* What We Can Learn from the Capital One Hack (Aug. 2, 2019), https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/ (last accessed Aug. 4, 2019).

[35] *Id*.

[36] *See* IAM Roles for Amazon EC2, https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html (last accessed August 1, 2019).

[37] *See* How the Accused Capital One Hacker Stole Reams of Data From the Cloud (Aug. 4, 2019), https://www.wsj.com/articles/how-the-accused-capital-one-hacker-stole-reams-of-data-from-the-cloud-11564911001?shareToken=sta69879a3c7c8434698050cd6ca996b4b&reflink=article_email_share (last accessed Aug. 5, 2019).

[h]owever, if several organizations all make similar configuration errors, it is time to ask whether the underlying [cloud] technology needs to be made safer, and whether the company that makes it shares responsibility of the breaches."[38]

69. Had the Amazon Defendants taken reasonable steps to mitigate the SSRF threat, such as whitelisting DNS names or IP addresses that an application needs to access, disabling unused URL schemas such as "https" or "http" if only one type of URL is used, and authentication on internal services, or, as Google has done, require a special "header" for metadata service requests,[39] the Capital One Data Breach could have been mitigated. Instead, the Amazon Defendants placed profits over data security and caused harm to consumers.

70. As a direct and proximate result of the Amazon Defendants' inadequate data security measures and failure to remediate this known exploit, Plaintiff and the Class suffered damages in the form of their PII being exposed.

E. Thompson Posted Consumers' PII on the Internet for Anyone to Access, Where it Sat for Three Months Before Capital Discovered the Breach

71. On April 21, 2019, Thompson posted consumers' PII that she illegally obtained through the Capital One Data Breach on the website "GitHub," a cloud-based service that helps developers store and manage their code.

72. In posting consumers' PII to GitHub, Thompson enabled anyone that clicked on her profile to access, view, and copy consumers' PII.

---

[38] *See* U.S. Senator Sends Letter to Amazon CEO on Capital One Hack, (Aug. 5, 2019), https://www.wsj.com/articles/u-s-senator-sends-letter-to-amazon-ceo-on-capital-one-hack-11565036507?shareToken=stf8b4e3995d76466d9fda21d7c8b1d1bd&reflink=article_email_share (last accessed Aug. 6, 2019).

[39] Preventing the Capital One Breach, https://ejj.io/blog/capital-one (last accessed Aug. 4, 2019).

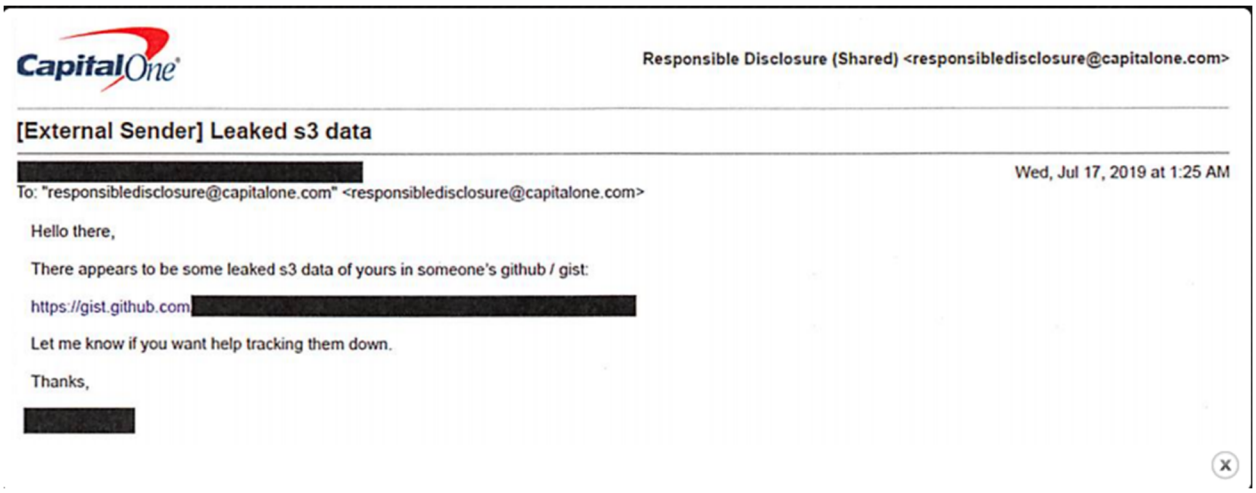
73. In doing so, Thompson opened the door for any malicious actor to view and obtain consumers' PII, making it likely that such information would result in identity theft or fraud to Plaintiff and the Class.

74. Capital One failed to detect the Capital One Data Breach and the GitHub post that contained consumers' PII for at least three months, despite having Information Technology systems engineers and a purported security policy in place to detect such intrusion into its network. Instead, consumers' PII sat on a public website, available to anyone to access, collect, and download, for three months.

75. During this time, Capital One failed to realize that its systems had been breached and that PII of over 100 million consumers had been compromised. Had Capital One been more responsive and proactive in identifying the breach, the scope and consequences of the intrusion could have been minimized. Instead, the delay contributed to the size of the breach and the resulting damages to Plaintiff and the Class.

76. Capital One was unaware of the data breach until July 17, 2019, when an individual emailed Capital One and alerted them that "[t]here appears to be some leaked s3 data of yours in someone's github / gist"[40]

[40] *See* Paige A. Thompson Criminal Complaint, Case No. MJ19-0344 ¶ 25 (W.D. Wash.), https://www.justice.gov/usao-wdwa/press-release/file/1188626/download.



Capital One

Responsible Disclosure (Shared) <responsibledisclosure@capitalone.com>

[External Sender] Leaked s3 data

[redacted] Wed, Jul 17, 2019 at 1:25 AM

To: "responsibledisclosure@capitalone.com" <responsibledisclosure@capitalone.com>

Hello there,

There appears to be some leaked s3 data of yours in someone's github / gist:

https://gist.github.com[redacted]

Let me know if you want help tracking them down.

Thanks,

[redacted]

77. Capital One then examined the GitHub file, and determined that the file contained the IP address for a specific server. It concluded that "[a] firewall misconfiguration permitted commands to reach and be executed by [a Capital One] server, which enabled access to folders or buckets of data in Capital One's storage space at the Cloud Computing Company."[41]

78. According to the FBI, the file contained "code for three commands, as well as a list of more than 700 folders or buckets of data."[42] It determined that the first command obtained security credentials that enabled access to certain Capital One folder at AWS; the second command listed the names of the folders or buckets of data in Capital One's storage space at AWS; and the third command extracted data from folders that those credentials had the requisite permissions to.[43]

79. Capital One determined that on or around March 12, 2019, Thompson initially attempted to access Capital One's data. It further determined that on March 22, 2019, the first and second command codes were used to list the names of the folders of Capital One data, and obtained "data from certain of Capital One's data folders or buckets, including files that contain credit card

[41] *Id.*
[42] *Id.*
[43] *Id.*

application data."[44] On April 21, 2019, Thompson again ran those commands and obtained the data that was ultimately posted to GitHub later that day.

80. In a June 16, 2019 tweet, Thompson described a method for gaining access to files stored on AWS S3 systems that appears to closely match the method used to access Capital One's data:

The Twitter user "erratic" posting about tools and processes used to access various Amazon cloud instances.

81. Thompson similarly stated in an online message "[d]ude so many people are doing it wrong," referring to how some companies were incorrectly configuring their servers.[45]

82. Significantly, the attack vector described by Thompson in her tweets is not limited to Capital One's systems. Rather, it exploits a general vulnerability of certain configurations of AWS' S3 systems generally using a widely known vulnerability of which the Amazon Defendants were aware and could have prevented or mitigated.

---

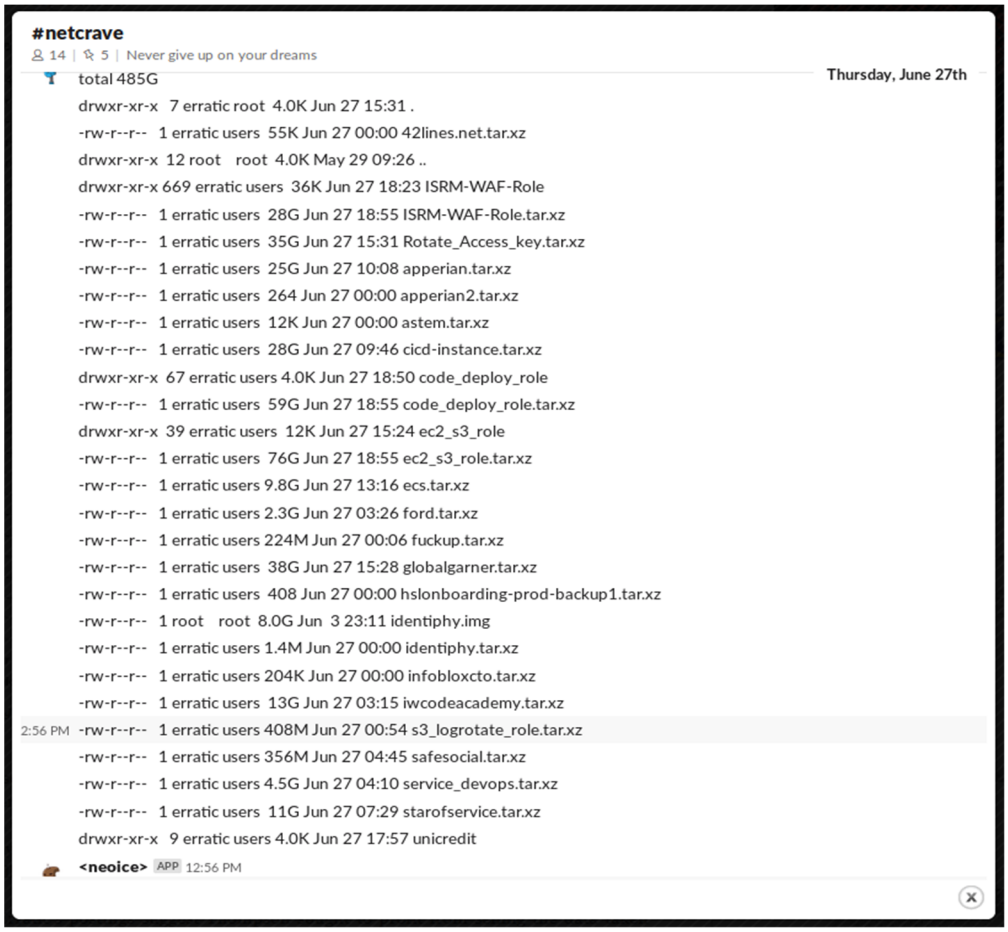
[44] *Id.*

[45] *See* How the Accused Capital One Hacker Stole Reams of Data From the Cloud (Aug. 4, 2019), https://www.wsj.com/articles/how-the-accused-capital-one-hacker-stole-reams-of-data-from-the-cloud-11564911001?shareToken=sta69879a3c7c8434698050cd6ca996b4b&reflink=article_email_share (last accessed Aug. 5, 2019).

83. It is likely that Thompson took advantage of this AWS configuration vulnerability to breach a number of other large corporations and organizations through the AWS network, including "one of the world's biggest telecom providers, an Ohio government body and a major U.S. university."[46]

84. Thompson posted additional comments in the public chatroom Slack on June 27, 2019, showing other viewers hundreds of gigabytes of files she had allegedly exfiltrated from various targets using the same AWS configuration vulnerability:

[46] *See* Thomas Brewster, *DOJ Says Capital One Mega Breach Suspect Could Face More Charges—Did She Hack Multiple Companies?*, Forbes (July 30, 2019), https://www.forbes.com/sites/thomasbrewster/2019/07/30/capital-one-mega-breach-suspectmay-have-hacked-many-more-companies (last accessed July 31, 2019); *see also* Paige A. Thompson Criminal Complaint, Case No. MJ19-0344 ¶ 25 (W.D. Wash.) ("I understand this post to indicate, among other things, that PAIGE A. THOMPSON intended to disseminate data from *victim entities, starting with Capital One*.") (emphasis added).



85. Despite publicly boasting of her achievements, Defendants did not discover the breach until four months after Thompson initially gained access to the breached data through the AWS configuration vulnerability, when an unknown third party emailed the Capital One Defendants on July 17, 2019.

F. Capital One and the Amazon Defendants Failed to Store PII in Accordance with Federal Regulations

86. The Federal Trade Commission (FTC) has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need

for data security should be factored into all business decision-making.[47] The FTC's recommended security measures include encrypting information stored on computer networks; holding on to information only as long as necessary; properly disposing of personal information that is no longer needed; limiting administrative access to business systems; using industry-tested and accepted security methods; monitoring network activity to uncover unapproved activity; verifying that privacy and security features work; testing for common vulnerabilities; and, updating and patching third-party software.[48]

87. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

88. Capital One's and the Amazon Defendants' failure to employ reasonable and appropriate security measures to protect against unauthorized access to confidential consumer data (i.e. PII) constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

89. Here, Capital One and the Amazon Defendants were at all times fully aware of their obligations to protect the personal and financial data of consumers. Capital One was aware of the

[47] Federal Trade Comm'n, Start With Security A Guide For Business, Lessons Learned from FTC Cases (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[48] *See id*.; Federal Trade Comm'n, Protecting Personal Information, A Guide For Business (Oct. 2016), https://www.ftc.gov/system/files/documents/plainlanguage/pdf-0136_proteting-personal-information.pdf.

significant consequences if it failed to do so because Capital One collected applicant data from millions of consumers and knew that this data, if hacked, would result in widespread injury to consumers. The Amazon Defendants similarly knew the importance of keeping data stored on its cloud secure, especially for financial institutions that entrusted it with personal and financial information of millions of consumers.

G. The Capital One Data Breach Will Lead to Increased Actual and Potential Identity Theft

90. The ramifications of Defendant's failure to keep consumers' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims can continue for years.

91. Identity theft occurs when someone uses another's personal and/or financial information such as that person's name, address, social security number, and other information, without permission, to commit fraud and other crimes.

92. Identity thieves can use personal information such as that pertaining to Plaintiff and the Class, which Capital One failed to keep secure, to perpetuate a variety of crimes that harm victims. Examples include filing a tax return using the victim's information to obtain a fraudulent refund, opening lines of credit in the victim's name, and obtaining medical treatments and procedures under false aliases. It is recognized by the US government and privacy experts that identity theft can take years to come to light or be detected.

93. The personal and financial information that Capital One failed to protect is "as good as gold" to thieves on the cyber black market, where thieves can use victims' personal data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts or clone ATM, debit, or credit cards.

94. A 2016 survey found that "[t]he quicker a financial institution, credit card issuer, . . . or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[49]

95. Capital One's delay in detecting and notifying consumers of the data breach has resulted in heightened risk of fraud for Plaintiff and the Class. In the case of compromised PII, identity theft victims must spend numerous hours researching, monitoring, remediating, and repairing potential and actual damage done to their credit. It is estimated that identity theft victims spend "an average of about 7 hours clearing up the issues" and resolving the consequences of fraud.[50] In extreme cases, victims can spend up to 1,200 hours resolving identity theft problems.[51]

96. As a direct and proximate result of Capital One's actions and inactions, Plaintiff and the Class have been placed in imminent, immediate and increased risk of harm from identity theft and fraud. Among other things, Plaintiff and the Class must attempt to prevent misuse of their PII, including reviewing and monitoring credit card statements for unusual or unknown charges, placing fraud alerts or credit freezes on credit bureau reports, and monitoring credit report for suspicious activity.

---

[49] *Identity Fraud hits Record high with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, https://www.javelinstrategy.com/pressrelease/identity-fraud-hits-record-high-154-million-us-victims-2016-percent-according-new, February 1, 2017.

[50] Victims of Identity Theft, 2014 (Sept. 2015) available at http://www.bjs.gov/content/pub/pdf/vit14.pdf

[51] *See* How Long Does it Take to Recover From Identity Theft?, available at https://www.lifelock.com/learn-identity-theft-resources-how-long-does-it-take-to-recover-from-identity-theft.html (last accessed Aug. 8, 2019).

97. Plaintiff and the Class now face years of vigilance regarding their personal and financial records. Plaintiff and the Class are incurring and will continue to incur such damages in addition to damages related to dealing with fraudulent credit and debit card charges and any resulting loss of use of their credit, regardless of whether such charges are ultimately reimbursed by banks or credit card companies.

H. Plaintiff and the Class Suffered Damages

98. The PII of Plaintiff and the Class are private, sensitive in nature, and now, exposed for misuse by identity thieves. Plaintiff and the Class entrusted Capital One with, and did not authorize the disclosure of, their PII except as required by law.

99. The Capital One Data Breach was the direct and proximate result of Capital One's and the Amazon Defendants' negligent failure to properly safeguard and protect Plaintiff's and the Class' PII from unauthorized access, use, and disclosure, in violation of federal regulations, industry best practices, and the common law, including Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and the Class' PII, to protect against reasonably foreseeable threats to the security integrity of such information, and to protect against known vulnerabilities in AWS' platform.

100. Capital One and the Amazon Defendants had the resources to prevent a breach yet failed to deploy those resources in a way that would have prevented the Capital One Data Breach from occurring.

101. Had Capital One remedied the deficiencies in its computer systems, followed federal and state regulations, and adopted security measures recommended by experts in the field,

it could have prevented intrusion into its computer systems and, ultimately, the theft of its consumers' confidential PII.

102. As a result of Capital One's and the Amazon Defendant's conduct, Plaintiff's and the Class' PII have been placed in imminent, immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to take the time to mitigate the actual and potential damages of the Capital One Data Breach, including monitoring credit reports, placing freezes with credit reporting agencies, and closely monitoring accounts for fraudulent activity.

I. Plaintiff's Interactions With Capital One

103. In or about August 2013, Plaintiff received letters in the mail from Capital One informing him that he was pre-qualified for Visa and MasterCard credit cards serviced by Capital One.

104. Plaintiff acted on Capital One's offer letters and went online to complete the credit card applications through Capital One's website.

105. On the website, Plaintiff was required to provide PII in order to be approved for the credit cards, including his name, date of birth, social security number, and home address, among other things.

106. Plaintiff provided the requisite PII to Capital One in order to complete the credit card applications.

107. Plaintiff entrusted Capital One with his PII with the expectation that it would store his PII in a safe manner consistent with state, federal and local laws, and in conformity with Capital One's Privacy Policy, which formed the basis of his agreement to provide his sensitive PII to Capital One.

108. Upon completion of the application, Plaintiff was approved for one MasterCard credit card and one Visa credit card.

109. Plaintiff continues to have these credit cards.

110. Upon information and belief, Plaintiff's PII has been compromised in the data breach announced by Capital One on July 29, 2019, and must now spend time remediating and monitoring his financial accounts and credit reports, among other things, due to the unauthorized disclosure of his PII.

V. CLASS ALLEGATIONS

111. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and c(4), Plaintiff seeks certification of the following nationwide class ("Class"):

> All persons in the United States whose PII was compromised in the Capital One Data Breach announced by Capital One on July 29, 2019.

112. Excluded from the Class are Defendants, its subsidiaries and affiliates; Defendants' employees; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

113. Plaintiff reserves the right to modify, expand or amend the above class definition or to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate following discovery.

114. **Numerosity**. Consistent with Rule 23(a)(1), the Class is so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiff believes that there approximately 100 million members in the Class based on the number of compromised accounts disclosed by Capital One. Class members may be identified through objective means, specifically by parsing through the files of data that were posted to GitHub by Thompson, which

are also in Capital One's custody. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

115. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether Defendants failed to adequately safeguard Plaintiff's and the Class members' PII;

b. Whether Defendants failed to keep Plaintiff's and the Class members' PII secure;

c. Whether Defendant's storage of Plaintiff's PII and the Class members' PII violated federal, state, local laws, or industry standards;

d. Whether Defendants engaged in unfair or deceptive practices by failing to properly safeguard Plaintiff's and the Class members' PII, as advertised and promised;

e. Whether reasonable security measures to monitor and detect unauthorized activity known and recommended by the FTC could have thwarted the data breach;

f. Whether Defendants' failure to implement adequate data security measures and remediate known issues within AWS' cloud storage platform allowed the data breach to occur;

g. Whether Defendants violated the consumer protection statutes applicable to Plaintiff and members of the Class;

h. Whether Defendants failed to notify Plaintiff and members of the Class about the Capital One Data Breach as soon as practical and without delay after the breach was discovered;

i. Whether Defendants acted negligently in failing to safeguard Plaintiff's and the Class members' PII;

j. Whether Plaintiff and members of the Class are entitled to damages as a result of Defendants' conduct; and

k. Whether Plaintiff and members of the Class are entitled to relief.

116. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff is a typical member of the Class. Plaintiff is an individual who applied for consumer credit with Capital One and voluntarily entrusted Capital One with their highly sensitive PII during the application process. Plaintiff and members of the Class sustained damages as a result of Defendants' uniform wrongful conduct during transactions with them, including their storage and transmission of the PII and failure to adequately safeguard it.

117. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Defendants to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff has also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated several data breach cases to successful results. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

118. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy,

and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system, create the potential of inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

VI. CAUSES OF ACTION

COUNT I

Negligence

(Against all Defendants on Behalf of Plaintiff and the Class)

119. Plaintiff realleges and incorporates by reference all preceding allegations as if set forth in this Count.

120. The Capital One and Amazon Defendants owed an independent duty to Plaintiff and members of the Class to take reasonable care in protecting their PII and to timely notify Plaintiff in the case of a data breach. This duty arises from multiple sources.

121. The Capital One and Amazon Defendants owe an independent, general duty of reasonable care to Plaintiff and the Class because it was foreseeable that hackers would target PII that financial institutions, such as the Capital One Defendants, and cloud storage companies, such

as the Amazon Defendants, routinely collect and store. It was also foreseeable that a hacker would extract PII from the Capital One Defendants' systems and misuse that information to the detriment of Plaintiff and the Class, and that Plaintiff and the Class would be forced to mitigate identity theft by monitoring their credit, freezing credit reports, and spending extra time closely monitoring accounts for fraudulent activity.

122. The Capital One and Amazon Defendants' common law duty also arises from the special relationship that exists between Defendants and the Class. Plaintiff and the Class entrusted Capital One with their sensitive PII in exchange for the prospect of obtaining credit through Capital One. The Amazon Defendants similarly agreed to keep such data safe and secure from unauthorized intrusion. The Capital One and Amazon Defendants, as keepers of that information, were the only parties that could realistically ensure that its data systems were sufficient to protect the data it was entrusted to hold.

123. In addition to the common law, Defendants also had a duty to take reasonable measures to protect consumers' PII pursuant to Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits unfair practices in or affecting commerce and requires the Capital One and Amazon Defendants to take reasonable security measures. The FTC publications and data security breach orders further form the basis of the Capital One and Amazon Defendants' duty to adequately protect sensitive PII. Moreover, several states have enacted statutes based upon the FTCA that also give rise to a duty of care.

124. The Capital One and Amazon Defendants are also obligated to conduct their business operations, including properly securing and storing data from external intrusion, in accordance with industry standards. Industry standards create yet another source of obligations that mandate Defendants to exercise reasonable care with respect to Plaintiff and the Class.

125. Defendants, by their actions, breached their duties to Plaintiff and the Class. Specifically, Defendants failed to act reasonably in protecting consumers' PII and di not have reasonably adequate security systems, procedures, and threat response monitoring or plans in place to prevent the disclosure and theft of consumers' PII.

126. The Capital One and Amazon Defendants also had the opportunity and resources to prevent a data breach. Capital One, as one of the largest banks in the United States, reports revenues in the billions of dollars annually. It easily could have spent sufficient money to ensure that an information technology infrastructure was in place that, at a minimum, guaranteed all firewalls were properly configured and being monitored by properly trained, and sufficiently staffed, personnel. Similarly, the Amazon Defendants, who jockey for the title of most valuable company in the world, could have spent sufficient resources to ensure data security and remediate known vulnerabilities on its cloud storage platform. Capital One and Amazon were fully aware of the possibility and consequences of a data breach of data stored in the cloud, and the FTC and other data security experts have provided guidance on how to enhance the security of its data systems. Both Defendants, however, failed to take such action and instead left its data systems unreasonably vulnerable to a breach.

127. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class members' PII has been compromised and is available for bad actors to illegally use. Plaintiff and the Class have suffered and continue to suffer injury, including but not limited to theft of personal and financial information, costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts and personal information, costs associated with the time spent and the loss of productivity related to mitigating, monitoring, and managing personal and financial account information in the wake of actual and future consequences of the data breach,

including purchasing credit monitoring and identity theft services and identifying fraudulent charges.

COUNT II

Negligence Per Se

(Against all Defendants on Behalf of Plaintiff and the Class)

128. Plaintiff realleges and incorporates by reference all preceding allegations as if set forth in this Count.

129. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted by the FTC, the unfair act or practices by businesses such as Capital One and Amazon of failing to use reasonable measures to protect cardholder data. The FTC publications and orders described herein also form the basis of Defendants' duty.

130. Defendants violated Section 5 of the FTCA by failing to use reasonable measures to protect PII and by not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it stored and the foreseeable consequences of a data breach, including decreased value of consumers' PII and time spent monitoring and protecting against identity theft.

131. Defendants' violation of Section 5 of the FTCA, and similar state statutes, constitutes negligence per se.

132. Plaintiff and the Class are within the class of persons Section 5 of the FTCA and similar state statutes were intended to protect. Additionally, the harm that occurred is the type of harm the FTCA and similar state statutes were intended to guard against. The FTC has pursued over fifty enforcement actions against businesses that, as a result of their failure to employ

reasonable data security measures and avoid unfair and deceptive practices, caused the harm suffered by Plaintiff and the Class.

133. Thus, it was reasonably foreseeable that Defendants' breaches of duties and failure to adequately safeguard consumers' PII would, and did, result in injuries to Plaintiffs, including theft of personal and financial information, costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts and personal information, costs associated with the time spent and the loss of productivity related to mitigating, monitoring, and managing personal and financial account information in the wake of actual and future consequences of the data breach, including purchasing credit monitoring and identity theft services and identifying fraudulent charges.

134. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class members' PII has been compromised and was made available for bad actors to illegally use. Plaintiff and the Class have suffered and continue to suffer injury, including but not limited to the actual and potential theft of personal and financial information, costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts and personal information, costs associated with the time spent and the loss of productivity related to mitigating, monitoring, and managing personal and financial account information in the wake of actual and future consequences of the data breach, including purchasing credit monitoring and identity theft services and identifying fraudulent charges.

COUNT III

Breach of Contract

(Against Capital One Defendants on Behalf of Plaintiff and the Class)

135. Plaintiff realleges and incorporates by reference all preceding allegations as if set forth in this Count.

136. Plaintiff and the Class entered into a contract with Capital One when they provided their PII in exchange for services, including access to and the use of credit. Capital One agreed to reasonably protect class members' PII.

137. Capital One solicited and invited members of the Class to provide sensitive and confidential PII as part of Capital One's standard business practices. Plaintiff and the Class accepted Capital One's offer and provided Capital One their PII in connection with its credit card applications.

138. In entering into such contracts, Plaintiff and the Class reasonably expected that Capital One would employ adequate data security measures and monitoring to keep their PII safe and secure from unauthorized access and intrusion consistent with applicable laws, regulations, industry standards, and their very own privacy policies.

139. Plaintiff and Class members reasonably expected and believed that Capital One would employ reasonable data security measures to keep their PII safe and secure. Capital One failed to do so.

140. Had Plaintiff and the Class known that Capital One would fail to employ reasonable means to safeguard their sensitive PII, Plaintiff and the Class would not have entered into an implied contract with Capital One to keep their PII reasonably safe and secure.

141. While Plaintiff and the Class upheld their end of the bargain with Capital One, Capital One failed to do so. Capital One breached its contracts with Plaintiff and the Class by failing to safeguard and protect their PII.

142. As a direct and proximate result of Capital One's breaches of contract, Plaintiff and the Class suffered damages as described in this Complaint.

143. Plaintiff and the Class are entitled to recover compensatory and consequential damages sustained as a result of this data breach.

144. Plaintiff and the Class also seek injunctive relief against Capital One, requiring Capital One to strengthen its data security measures, submit future audits of its data security efforts and procedures, and provide Plaintiff and the Class with free credit report monitoring and identity theft insurance.

COUNT IV

Breach of Implied Contract

(Against the Capital One Defendants on Behalf of Plaintiffs and the Class)

145. Plaintiff realleges and incorporates by reference all preceding allegations as if set forth in this Count.

146. Capital One solicited Plaintiff and the Class to apply for and obtain credit services from Capital One. Plaintiff and the Class accepted Capital One's invitation to apply for credit and did, in fact, apply for credit. As part of the application process, Capital One required Plaintiff and the Class to furnish their PII in order to determine creditworthiness. In doing so, Plaintiff and the Class entered into implied contracts with Capital One, under which Capital One undertook and agreed to safeguard and protect applicant-consumers' PII.

147. The use of Capital One credit products or services was based on the mutually agreed upon implied contract between Capital One and consumers wherein Capital One agreed to safeguard and protect Plaintiff's and the Class' sensitive PII and financial information.

148. Plaintiff and the Class would not have provided their sensitive PII and financial information to Capital One without the implies contract between them.

149. At all times, Plaintiffs and members of the Class upheld their obligations under the implied contract with Capital One.

150. Capital One breached the implied contracts with Plaintiff and the Class when it failed to safeguard and protect their sensitive PII and financial information.

151. As a direct and proximate result of Capital One's breaches of the implied contracts, Plaintiffs and members of the Class sustained injury as described in this Complaint.

COUNT V

Violations Of Minnesota's Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44

(Against all Defendants on Behalf of Plaintiff and the Class)

152. Plaintiff realleges and incorporates by reference all preceding allegations as if set forth in this Count.

153. Minnesota's Uniform and Deceptive Trade Practices Act, Minn. Stat. § 325D.44, *et seq.* (MNDTPA) prohibits any person from engaging in deceptive trade practices which "represents that goods or services have . . . characteristics, ingredients, uses, benefits. . . they do not;. . . [or] engages in any other conduct which similarly creates a likelihood of confusion or misunderstanding" Minn. Stat. § 325D.44, subd. 1(5), (13).

154. Defendants' actions violated Minn. Stat. § 325D.44. Specifically, Defendants omitted the fact at the time they solicited Plaintiff and the Class, and at all relevant times thereafter, that they failed to take reasonable steps to protect sensitive PII entrusted to and stored by them.

155. Defendants' omissions had the capacity to deceive, and did deceive, Plaintiff and the Class.

156. Defendants undertook an obligation to keep Plaintiff's and the Class' sensitive PII safe, secure, and free of unauthorized access and dissemination. Defendants were therefore responsible for implementing security procedures that would achieve as much and should have known that the measures in place failed to adequately protect consumers' PII. Defendants' conduct was deceptive because it failed to offer the degree of protection mandated by applicable laws, regulations, industry standards, and their very own privacy policies, despite the fact that Defendants held themselves out to the public as employing reasonable data security measures.

157. Had Plaintiff and the class known that Defendants' data security measures did not comport with their representations, Plaintiff and the Class would not have provided their PII to Defendants.

158. As a result of Defendants' conduct, Plaintiff and the Class sustained damages as alleged herein. Plaintiff are entitled to recover damages, equitable, and injunctive relief, including attorneys' fees and costs, as permitted pursuant to Minn. Stat. § 325D.45, subd. 2.

COUNT VI

Violations of Minnesota's Prevention of Consumer Fraud Act, Minn. Stat. § 325F.69

(Against the Capital One Defendants on Behalf of Plaintiff and the Class)

159. Plaintiff realleges and incorporates by reference all preceding allegations as if set forth in this Count.

160. Minn. Stat. § 325F.69 Subd. 1 provides:

> The act, use, or employment by any person of fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is enjoined as provided in section 325F.70.

161. Capital One sells consumer credit, which falls within the meaning of "merchandise" under Minn. Stat. § 325F.68, subd. 2.

162. Defendant's misrepresentations, misleading statements, and deceptive practices of offering Plaintiff and the Class credit in exchange for sensitive PII without informing them that their data security measures did not conform to applicable laws, regulations, industry standards, and their very own privacy policies constitutes the use of fraud, false pretenses, and deceptive practices, and thereby results in multiple violations of Minn. Stat. § 325F.69.

163. Defendant's material omissions constitute deceptive conduct that violated Minn. Stat. § 325F.69. Specifically, at the time Plaintiff accepted Defendants' credit offers, Defendant omitted the fact that it failed to take reasonable steps to protect the security of consumers' sensitive PII entrusted to them.

164. These omitted facts were material in that a reasonable consumer would not have agreed to provide sensitive PII to Defendant in exchange for consumer credit had they known that reasonable data security measures were not in place.

165. Defendant intended that Plaintiff and the Class rely upon the misleading statements made in its privacy policy concerning the data security measures employed to protect consumers' PII in violation of Minn. Stat. § 325F.69.

166. As a result of Defendants' misconduct, Plaintiff and the Class have suffered damages and are entitled to injunctive and equitable relief, including, but not limited to, restitution, disgorgement, and an award of attorneys' fees pursuant to Minn. Stat. § 8.21, subd. 3a.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and the Class they seek to represent, respectfully request that this Court enter an Order:

1. Certifying this case as a class action on behalf of Plaintiff and the Class defined above, appointing Plaintiff as Class Representative of the Class, and appointing Plaintiff's counsel to represent the Class;

2. Awarding Plaintiff and the Class appropriate relief, including actual and statutory damages;

3. Awarding equitable, injunctive, and declaratory relief as may be appropriate, including, without limitation, an injunction and declaring Defendants' conduct to be unlawful;

4. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

5. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowed by law;

6. Permitting Plaintiff and the Class to amend their pleadings to conform the evidence produced at trial; and

7. Awarding such other and further relief as equity and justice may require.

JURY DEMAND

Plaintiff respectfully requests a trial by jury.

DATED: August 13, 2019

Respectfully submitted,

/s/ *Peter C. Grenier*
Peter C. Grenier (VSB # 50997)
GRENIER LAW GROUP PLLC
1920 L Street, N.W. Suite 750
Washington, D.C. 20005
Telephone: (202) 768-9600
Facsimile: (202) 768-9604
pgrenier@grenierlawgroup.com

Brian C. Gudmundson (*Pro Hac Vice* Pending)
Bryce D. Riddle (*Pro Hac Vice* Pending)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 641-0844
brian.gudmundson@zimmreed.com
bryce.riddle@zimmreed.com

Bryan L. Bleichner (*Pro Hac Vice* Pending)
CHESTNUT CAMBRONNE PA
17 Washington Avenue North, Suite 300
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612) 336-2940
bbleichner@chestnutcambronne.com